United States District Court
Northern District of California

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

FINJAN, INC.,
Plaintiff,
v.
SONICWALL, INC.,
Defendant.

Case No.17-cv-04467-BLF (VKD)

ORDER RE MOTION TO COMPEL FURTHER SUPPLEMENTAL INFRINGEMENT CONTENTIONS

Re: Dkt. No. 112

Finjan, Inc. ("Finjan") sues defendant SonicWall, Inc. ("SonicWall") for patent infringement. SonicWall moves to compel Finjan to provide further supplemental infringement contentions. Dkt. No. 112. This motion was referred to the undersigned judge. Dkt. No. 75. The Court heard oral argument on the motion on March 12, 2019. Dkt. No. 128. Having considered the parties' briefs and arguments made at the hearing, the Court grants SonicWall's motion to compel as described below.

I. BACKGROUND

On April 10, 2018, Finjan served its original disclosure of asserted claims, infringement contentions, and document production pursuant to Patent Local Rules 3-1 and 3-2. The original disclosure asserted infringement of 39 claims across the following ten patents: U.S. Patent Nos. 6,154,844 ("the '844 patent"); 7,058,822 ("the '822 patent"); 6,804,780 ("the '780 patent"); 7,613,926 ("the '926 patent"); 7,647,633 ("the '633 patent"); 8,141,154 ("the '154 patent"); 8,677,494 ("the '494 patent"); 7,975,305 ("the '305 patent"); 8,225,408 ("the '408 patent"); and 6,965,968 ("the '968 patent"). *See* Dkt. No. 112-2 at 2. After SonicWall objected to deficiencies in the original disclosure, Finjan served a supplemental disclosure on November 9, 2018, in which it added approximately 500 pages of excerpts from recently produced confidential SonicWall documents. Dkt. No. 118 at 2; c*ompare* Dkt. No. 112-2 at 1 (stating that Finjan's original disclosures amounted to "over 1,400 pages of contentions") *with* Dkt. No. 118-2 ¶ 10 ("On November 9, 2018, Finjan served supplemental infringement contentions, with charts totaling over 1900 pages.").

Finjan's supplemental disclosure includes a cover pleading that identifies the asserted claims, provides a summary of Finjan's infringement contentions, and describes the documents Finjan has produced in support of its assertions. The cover pleading attaches a list of accused instrumentalities and 31 claim charts. Dkt. No. 112-3. The list of accused instrumentalities includes at least 99 distinct instrumentalities—software and hardware products and services—organized into three product categories: (1) SonicWall Gateways, (2) SonicWall Email Security Appliance (ESA) products, and (3) Secure Mobile Access (SMA) Appliance products. *Id.*, Ex. A at 1–2. Finjan separately identifies SonicWall's Capture Advanced Threat Protection ("Capture ATP") product as an accused instrumentality, but also includes it within each of the three identified product categories. *Id*.

SonicWall now moves to compel further supplemental infringement contentions as to all asserted patents.

II. LEGAL STANDARD

Patent Local Rule 3-1 requires, among other things:

> [A] party claiming patent infringement shall serve on all parties . . . the "Disclosure of Asserted Claims and Infringement Contentions" [which] shall contain the following information:
>
> > (a) Each claim of each patent in suit that is allegedly infringed by each opposing party, including for each claim the applicable statutory subsections of 35 U.S.C. § 271 asserted;
> >
> > (b) Separately for each asserted claim, each accused apparatus, product, device, process, method, act, or other instrumentality ("Accused Instrumentality") of each opposing party of which the party is aware. This identification shall be as specific as possible. Each product, device, and apparatus shall be identified by name or model number, if known. Each method or process shall be identified by name, if known, or by any product, device, or apparatus which, when used, allegedly results in the practice of the claimed method or process;

> (c) A chart identifying specifically where and how each limitation of each asserted claim is found within each Accused Instrumentality, including for each limitation that such party contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or material(s) in the Accused Instrumentality that performs the claimed function.
> . . .

"The overriding principle of the Patent Local Rules is that they are designed [to] make the parties more efficient, to streamline the litigation process, and to articulate with specificity the claims and theory of a plaintiff's infringement claims." *Bender v. Maxim Integrated Prods.*, No. 09-cv-01152-SI, 2010 WL 1135762, at *2 (N.D. Cal. Mar. 22, 2010) (alteration in original; internal citation omitted). Patent Local Rule 3-1 is intended to require the plaintiff "to crystallize its theories of the case early in the litigation and to adhere to those theories once disclosed." *Bender v. Advanced Micro Devices, Inc.*, No. 09-cv-1149-EMC, 2010 WL 363341, at *1 (N.D. Cal. Feb. 1, 2010). It "takes the place of a series of interrogatories that defendants would likely have propounded had the patent local rules not provided for streamlined discovery." *Network Caching Tech., LLC v. Novell, Inc.*, No. 01-cv-2079-VRW, 2002 WL 32126128, at *4 (N.D. Cal. Aug. 13, 2002).

"[A]ll courts agree that the degree of specificity under [Patent] Local Rule 3-1 must be sufficient to provide reasonable notice to the defendant why the plaintiff believes it has a 'reasonable chance of proving infringement.'" *Shared Memory Graphics LLC v. Apple, Inc.*, 812 F. Supp. 2d 1022, 1025 (N.D. Cal. 2010) (quoting *View Eng'g, Inc. v. Robotic Vision Sys., Inc.*, 208 F.3d 981, 986 (Fed. Cir. 2000)). The local rules do not "require the disclosure of specific evidence nor do they require a plaintiff to prove its infringement case," but "a patentee must nevertheless disclose what in each accused instrumentality it contends practices each and every limitation of each asserted claim to the extent appropriate information is reasonably available to it." *DCG Sys. v. Checkpoint Techs., LLC*, No. 11-cv-03792-PSG, 2012 WL 1309161, at *2 (N.D. Cal. Apr. 16, 2012).

III. DISCUSSION

SonicWall moves to compel further supplemental infringement contentions on three grounds. First, SonicWall says Finjan's contentions generally fail to identify the accused instrumentalities with sufficient specificity. Second, SonicWall says that the infringement contentions generally rely on screenshots without any explanation of how those screenshots disclose where a limitation may be found in an accused instrumentality. Third, SonicWall objects to specific alleged deficiencies in Finjan's charts for the '305, '926, '408, '844, '780, '154, and '968 patents.

A. Issues Common to All Asserted Patents

1. Finjan's Identification of Accused Instrumentalities

SonicWall argues that Finjan does not adequately identify the instrumentalities that Finjan contends infringe the asserted claims. SonicWall points to three problems: First, SonicWall says that Finjan's list of accused instrumentalities is insufficiently precise because it includes unidentified components, including "all supporting server and/or cloud infrastructure, Capture ATP, feeds, and other components that are utilized by" the specifically identified products. Dkt. No. 112-3, Ex. A at 1–2. Second, SonicWall says Finjan's claim charts contain open-ended descriptions of the accused instrumentalities, using phrases like "at least the following" and "either alone or when used in conjunction with" that encompass an unknown and undefined set of additional products and systems. Dkt. No. 112 at 6–7. Third, SonicWall says that Finjan relies on confusing alternative infringement "scenarios" that Finjan says infringe "either alone or in combination with Capture ATP," when Capture ATP is separately listed as *part of* the accused instrumentalities. *Id.* at 7.

SonicWall's complaints are well-taken. As currently drafted, Finjan's contentions do not provide SonicWall reasonable notice of what is actually accused. The use of open-ended language and references to other unidentified components renders Finjan's disclosure of the accused instrumentalities unacceptably vague. *See Finjan Inc. v. Proofpoint Inc.*, No. 13-cv-05808-HSG, 2015 WL 1517920, at *5–6 (N.D. Cal. Apr. 2, 2015) (limiting claims to products expressly named in infringement contentions and striking "including but not limited to" from Finjan's definition of "Proofpoint Products"); *Alacritech Inc. v. CenturyLink, Inc.*, No. 2:16-cv-00693-JRG-RSP, 2017 WL 3007464, at *2–3 (E.D. Tex. July 14, 2017) (rejecting catch-all language identifying accused instrumentalities as, among other things, "any of its other activities, products and/or services that use servers or computers to practice and/or support infringing LSO functionality" because such language fails to provide adequate notice of the allegedly infringing devices).

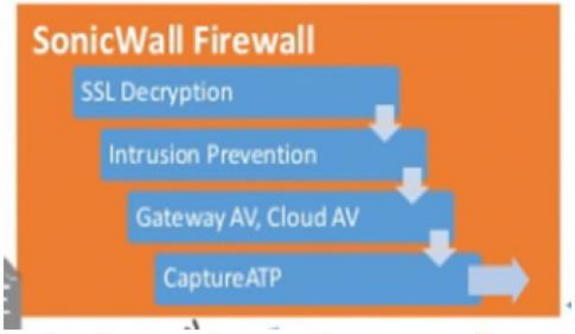
At the hearing, Finjan offered to revise its contentions to eliminate "and/or" language from its charts and to clarify that the "all supporting server and/or cloud infrastructure, Capture ATP, feeds, and other components that are utilized by" language is limited to the supporting server and/or cloud infrastructure described in Finjan's charts. Those revisions are necessary, but not sufficient. Finjan must amend its identification of accused instrumentalities to remove placeholder references to unspecified products, services, or components. In addition, Finjan must specify whether a product or service infringes alone or in combination. For example, if Finjan contends that the Capture ATP product infringes an asserted claim, both alone and in combination with some other product or service, its infringement contentions should make that clear. In addition, Finjan must avoid the confusion that arises from defining Capture ATP as both part of and separate from another accused instrumentality. *See Finjan, Inc. v. Check Point Software Techs., Inc.*, No. 18-cv-02621-WHO, 2019 WL 955000, at *4 (N.D. Cal. Feb. 27, 2019) (requiring Finjan to specify infringing combinations.)

2. Finjan's Use of Screenshots

SonicWall argues that Finjan's contentions do not satisfy the requirements of Patent Local Rule 3-1 because they refer extensively to screenshots of images taken from SonicWall marketing materials, with little or no explanation of how the information contained in the screenshots relates to the claim limitations at issue. As an example, SonicWall cites a portion of Finjan's infringement contentions for the "rule-based content scanner" limitation of claim 1 of the '305 patent, in which Finjan states:

> In one scenario, as shown below, the cloud AV scan engine (rule-based content scanner) of the SonicWall Gateways (network interface) scans the content of files transmitted through traffic that is inspected for parsing by a software proxy. The cloud AV scan engine communicates with the database of parser and analyzer rules when it queries the database to compare the content properties of the file being scanned against the content of recognizable computer exploits in order to identify the presence of potential computer exploits within the scanned file.

Dkt. No. 111-20 at 18. This text is followed by a screenshot:



Id. Finjan does not indicate where in the image any of the elements described in the text may be found, and it is by no means self-evident from the image alone. *See Digital Reg of Texas, LLC v. Adobe Sys. Inc.*, No. CV 12–01971–CW, 2013 WL 3361241, at *4 (N.D. Cal. July 3, 2013) (rejecting unexplained reference to screenshots in lieu of explanatory text); *Proofpoint*, 2015 WL 1517920, at *6 (same).

Patent Local Rule 3-1(c) requires Finjan to provide contentions "that identify what structure, act, or material in each of the [accused instrumentalities] infringes each claim element" by mapping each claim element to specific elements of the accused instrumentalities. *Proofpoint*, 2015 WL 1517920, at *6–7. Finjan correctly observes that there is no prohibition on the use of screenshots in infringement contentions. However, if Finjan wishes to rely on screenshots, it must identify how what is shown in the image maps to the particular claim limitation for which the image is referenced, such as by circling or labeling in a meaningful way the elements of the image that correspond to the limitations at issue.

Finjan must amend its contentions to eliminate the use of unexplained screenshots.

B. '305 Patent

The '305 patent is directed to a computer security system for scanning and diverting incoming content received from the Internet to an Internet application running on a computer. Dkt. No. 1-9. Claims 1 and 6 recite:

> 1. A security system for scanning content within a computer, comprising:
>
> > a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer;

> a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type;
>
> a rule-based content scanner that communicates with said database of parser and analyzer rules, operatively coupled with said network interface, for scanning incoming content received by said network interface to recognize the presence of potential computer exploits therewithin;
>
> a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content scanner; and
>
> a rule update manager that communicates with said database of parser and analyzer rules, for updating said database of parser and analyzer rules periodically to incorporate new parser and analyzer rules that are made available.
>
> 6. The system of claim 1 wherein the incoming content received from the Internet by said network interface is HTTP content.

Id. at claims 1, 6. SonicWall argues that Finjan does not identify the specific components in the accused instrumentalities that map to certain limitations of claim 6.

1. "a network interface housed within a computer"

SonicWall says that Finjan's contentions for the accused Capture ATP instrumentality do not identify "the computer" that houses the "network interface," as recited in claim 6. Finjan's contentions state that "[t]he computer which houses the network interface resides (either alone or as a distributed computer system) includes the Capture ATP and the Cloud Sandbox computers," and reference a diagram of Capture ATP. *See* Dkt. No. 111-22 at 1. Apart from the open-ended nature of this contention, the problem is that Finjan nowhere identifies what "the Capture ATP and Cloud Sandbox computers" are, and no such computers are identified in the referenced diagram.

Finjan must amend its contentions to identify where the computer that houses the network interface of claim 6 may be found in the accused Capture ATP instrumentality.

2. "database of parser and analyzer rules"

SonicWall says that Finjan's contentions for the accused Capture ATP instrumentality do not identify the "database of parser and analyzer rules," as recited in claim 6. Additionally, SonicWall contends that the database of parser and analyzer rules must be stored on the same computer that houses the network interface, and it complains that it cannot tell which, if any, component of Capture ATP is "the computer" of claim 6. Dkt. No. 112 at 10. Finjan responds that its contentions state that the database "resides on the Capture ATP system" and more specifically that "in some scenarios . . . the database or rules are stored in the SonicWall Firewall, SonicWall Capture cloud service, and/or the SonicWall GRID Data Center" within the Capture ATP system. Dkt. No. 118 at 9.

While Finjan has identified multiple locations where the database may be stored, it has not identified what element of Capture ATP constitutes the database of claim 6. Finjan must identify *the computer* on which the database is stored. In addition, if SonicWall has already produced technical documents, source code, and internal source code architecture documents for Capture ATP, Finjan should be in a position to also identify the database that meets this limitation. *DCG Sys.*, 2012 WL 1309161, at *2 ("[A] patentee must nevertheless disclose what in each accused instrumentality it contends practices each and every limitation of each asserted claim to the extent appropriate information is reasonably available to it."); *Check Point*, 2019 WL 955000, at *6 ("It is Finjan's obligation to identify the particular claim components in each claim, map those components onto the features of the allegedly infringing products, and pinpoint cite source code that practices that component."); *Proofpoint*, 2015 WL 1517920, at *6–7 (finding contentions, "largely comprised of generic marketing literature and screenshots" with only "high-level generalities" do not satisfy a patentee's burden under Patent L.R. 3-1(c)).

3. "Internet application running on a computer"

SonicWall says that Finjan's contentions for the Gateways, ESA, and Capture ATP instrumentalities do not identify any component that constitutes an "Internet application running on the computer," as recited in claim 6. Finjan responds that its contentions identify "web browsers, FTP or file download clients, messaging clients and email client applications" as "Internet applications." Dkt. No. 111-20 at 1; Dkt. No. 111-22 at 1; Dkt. No. 111-24 at 1. In addition, Finjan contends that the accused instrumentalities "include[] both hardware (such as a network interface) and software (proxy software) components that can receive content included in files (incoming content from the Internet on its destination to an Internet application running on the computer) for inspection to detect the presence of malware (a security system)[,]" and that they "include a network interface housed within a computer because they include both hardware and software components that scan content included in files transmitted between a source computer (e.g., Internet) and a destination computer (e.g., web client or application) over a computer network." Dkt. No. 111-20 at 1, 2; Dkt. No. 111-22 at 1, 2; Dkt. No. 111-24 at 1, 2.

These contentions are not sufficiently specific. Finjan identifies types of internet applications, but they are disclosed as *examples* only. Finjan does not identify any particular application or applications as the "Internet application running on the computer" that meets this limitation of claim 6. To the extent Finjan contends that the SonicWall Gateways or ESA products themselves are the "Internet application running on the computer," such contention is not clearly stated.

Finjan must amend its contentions to identify the Internet application or applications that meet this limitation of claim 6. If SonicWall has already produced technical specifications and source code for the Gateways, ESA, and Capture ATP products, Finjan should be able to identify the application or applications with specificity.

4. "rule-based content scanner"

SonicWall says that Finjan's contentions do not identify a "rule-based content scanner" for any accused instrumentality. In particular, SonicWall objects to Finjan's use of the undefined and unexplained terms "scan engine" and "scanners" as proxies for a specific component of the accused instrumentalities that meets this claim limitation when no such components with those names are identified in any of SonicWall's products. Dkt. No. 112 at 11–12. In addition, SonicWall complains that Finjan's contentions merely paraphrase the claim language without identifying the elements of the accused instrumentalities that perform the functions of the rule-based content scanner. Dkt. No. 120 at 7. Finjan responds that it has identified numerous items in the accused instrumentalities, including "AV scan engines, scanners using Yara rules, scanners using SonicWall Signatures, cache lookup, static analysis, sandbox, dynamic analysis, packet inspectors, or similar scan engine/analyzers," that perform the claimed functions of a rule-based content scanner. Dkt. No. 118 at 10.

The primary difficulty with Finjan's contentions here is that while all of these "scanners" may be *examples* of rule-based content scanners, it not clear whether Finjan contends that such scanners are, in fact, found in the accused instrumentalities, and if so, where they are found. It is not sufficient for Finjan to simply declare that a component that performs the claimed functionality exists in an accused instrumentality; Finjan must identify the infringing element and where it is found.

Finjan must amend its contentions to identify which component or components comprise the rule-based content scanner of claim 6. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed scanner with specificity.

5. "rule update manager"

SonicWall says that Finjan's contentions do not identify a "rule update manager" for any accused instrumentality. The parties' arguments with respect to this limitation are similar to the arguments they made with respect to the "rule-based content scanner" limitation.

The Court's decision is also the same. Finjan must amend its contentions to identify which component or components comprise the rule update manager of claim 6. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed rule update manager with specificity.

6. "patterns of types of tokens"

As recited in claim 6, the parser and analyzer rules stored in the database "describe computer exploits as patterns of types of tokens." SonicWall says that Finjan has not identified any aspect of the accused instrumentalities that constitutes rules describing exploits as "patterns of *types* of tokens," but has instead merely identified "tokens" or "token patterns." Dkt. No. 112 at 13 (emphasis original). SonicWall contends that this is an important distinction in view of the prosecution history of the '305 patent, in which the USPTO accepted Finjan's argument that its invention was not unpatentable in view of the prior art under 35 U.S.C. §§ 102(e) and 103(a) on the basis that "patterns of types of tokens" differs from "tokens." Dkt. No. 112-17 at 9 ("Applicants wish to point out that the phrases 'tokens' and 'patterns of types of tokens' have different meanings."). Finjan argued during prosecution that, "[i]n particular, as used in the subject specification, 'types of tokens' refers to a categorization of tokens into types. A 'type' is a category." *Id.*

Finjan's contentions refer almost exclusively to "tokens," "patterns," or "token patterns" in the accused instrumentalities. For example, Finjan's contentions for the SonicWall Gateways instrumentalities state:

> AV databases used by SonicWall Gateways contain parser and analyzer rules because the rules include conditions configured to recognize **patterns** that correspond to code associated with polymorphic viruses (obfuscated code), worms, Trojans, and malware (computer exploits). . . . The portions of program code used to produce the Polymorphic viruses, worms, Trojans, and malware are **tokens** because they are generated in accordance with the lexical constructs of a particular programming language so that they can be downloaded / executed at a destination computer, as intended by the code's author. The AV database includes analyzer rules because it stores **token patterns** that enable SonicWall Gateways to quickly detect program code associated with Polymorphic viruses, worms, Trojans, and malware when processing the code during file inspection procedures.

Dkt. No. 111-20 at 6 (emphases added); *see also* Dkt. No. 111-24 at 7 (same paragraph for ESA products). Finjan does not point to parser and analyzer rules in the Gateways instrumentalities that it says describe "patterns of types of tokens," except in summarizing its conclusion that the accused instrumentalities meet the claim limitation. *See, e.g.*, Dkt. No. 111-20 at 7 ("In [this] fashion, the parser and analyzer rules used by SonicWall Gateways describe these computer exploits as patterns of types of tokens based on the different character combinations."); *see also* Dkt. No. 111-24 at 9 (same paragraph for ESA products).

Finjan objects that SonicWall improperly attempts to argue claim construction issues in support of its motion to compel. Dkt. No. 118 at 13. Finjan also argues that its contentions are sufficiently detailed to put SonicWall on notice of what Finjan contends meets the "patterns of types of tokens" limitation. *Id.* at 13–14.

This dispute presents a closer call. Finjan has disclosed what it contends are tokens and patterns of tokens that are recognized by parser and analyzer rules. If Finjan believes that these tokens and patterns of tokens meet the "patterns of types of tokens" limitation, then no amendment is required, and SonicWall will be free to argue, in view of the prosecution history or otherwise, that tokens and patterns of tokens do not meet this limitation and the accused instrumentalities do not infringe on this basis. If, however, Finjan contends that the parser and analyzer rules recognize something other than tokens or patterns of tokens as "patterns of types of tokens," Finjan must disclose what that something else is. *See, e.g., St. Clair Intellectual Prop. Consultants, Inc. v. Matsushita Elec. Indus. Co., Ltd.*, C.A. Nos. 04-1436-LPS, 06-404-LPS, 08-371-LPS, 2012 WL 1015993, at *5 (D. Del. Mar. 26, 2012) ("When claim construction remains an open issue at the time the parties serve expert reports and infringement contentions, the parties have an obligation to prepare for the fact that the court may adopt the other party's claim construction.") (internal quotation marks and alterations omitted), *aff'd* 552 F. App'x 915 (Fed. Cir. 2013) (per curiam).

C. '926 Patent

The '926 patent is directed to a system for detecting malicious information associated with a downloadable application. Asserted claim 22 of the '926 patent claims a system for managing "Downloadables" as follows:

> 22. A system for managing Downloadables, comprising:
>
> a receiver for receiving an incoming Downloadable;
>
> a Downloadable identifier for performing a hashing function on the incoming Downloadable to compute an incoming Downloadable ID;
>
> a database manager for retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on the incoming Downloadable ID, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable; and
>
> a transmitter coupled with said receiver, for transmitting the incoming Downloadable and a representation of the retrieved Downloadable security profile data to a destination computer, via a transport protocol transmission.

Dkt. No. 1-5 at claim 22. The Court has adopted the parties' agreed construction of

"Downloadable" as meaning "an executable program, which is downloaded from a source computer and run on the destination computer." Dkt. No. 132 at 5. The parties dispute the adequacy of Finjan's contentions for two limitations of claim 22.

1. "database manager"

SonicWall says that Finjan's contentions do not identify any specific component within the accused instrumentalities that corresponds to the "database manager" that "retriev[es] security profile data for the incoming Downloadable." Instead, SonicWall says that Finjan relies on "functional claiming" in which it merely parrots the claim language. Dkt. No. 112 at 14–15. SonicWall also objects to Finjan's frequent reference to various scenarios in which Finjan says the database manager "includes" different SonicWall products or services. *Id.* Finjan responds that it has described in detail how the database manager infringes. *See* Dkt. No. 118 at 14. Finjan does not address SonicWall's principle objection, which is that Finjan has not identified which components of the accused instrumentalities constitute the claimed database manager.

Finjan's contentions for this limitation suffer from the same problems as many of its other contentions, as Finjan appears to rely on open-ended language and ambiguous references to screenshots to support its contention that the accused instrumentalities include the claimed database manager. Finjan does not state what component in any instrumentality *is* the database manager. It must amend its contentions to identify which component or components comprise the database manager of claim 22. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed database manager with specificity.

2. "database of Downloadable security profiles indexed according to Downloadable IDs"

SonicWall says that Finjan has effectively identified every database in the accused instrumentalities as the "database of Downloadable security profiles indexed according to Downloadable IDs," and so has not really identified any specific database or databases, thereby concealing its infringement theory from SonicWall. Dkt. No. 112 at 15–16. Finjan responds that its contentions do refer to specific databases and do not encompass databases that may only be used with an accused instrumentality. Dkt. No. 118 at 15.

Finjan has identified some specific databases that it contends are the claimed database of Downloadable security profiles indexed according to Downloadable IDs, but its contentions suffer from the problem of reliance on open-ended language discussed above. Finjan must amend its infringement contentions to identify the specific databases that it contends constitute the claimed database of Downloadable security profiles indexed according to Downloadable IDs of claim 22. Finjan's amended contentions also should disclose the basis for its contention that a particular database includes "Downloadable security profiles indexed according to Downloadable IDs." If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed database with specificity.

D. '408 Patent

The '408 patent is directed to a method and system for rule-based content scanning that identifies patterns of lexical constructs for a specific language and identifies the presence of potential exploits within an incoming byte stream based on rules for that language. Dkt. No. 1-10. Asserted claim 9 reads:

> 9. A computer system for multi-lingual content scanning, comprising:
>
> > a non-transitory computer-readable storage medium storing computer-executable program code that is executed by a computer to scan incoming program code;
> >
> > a receiver, stored on the medium and executed by the computer, for receiving an incoming stream of program code;
> >
> > a multi-lingual language detector, stored on the medium and executed by the computer, operatively coupled to said receiver for detecting any specific one of a plurality of programming languages in which the incoming stream is written;
> >
> > a scanner instantiator, stored on the medium and executed by the computer, operatively coupled to said receiver and said multi-lingual language detector for instantiating a scanner for the specific programming language, in response to said determining, the scanner comprising:
> >
> > > a rules accessor for accessing parser rules and analyzer rules for the specific programming

> language, wherein the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and wherein the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious;
>
> a tokenizer, for identifying individual tokens within the incoming;
> a parser, for dynamically building while said receiver is receiving the incoming stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules accessed by said rules accessor; and
>
> an analyzer, for dynamically detecting, while said parser is dynamically building the parse tree, combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules; and
>
> a notifier, stored on the medium and executed by the computer, operatively coupled to said scanner instantiator for indicating the presence of potential exploits within the incoming stream, based on results of said analyzer.

Id. at claim 9. SonicWall contends that Finjan has not identified the components in the accused instrumentalities that correspond to several limitations in claim 9.

1. “multi-lingual language detector”

SonicWall says that Finjan’s contentions do not identify any specific component in the accused instrumentalities that serves as a “multi-lingual language detector.” Instead, SonicWall argues, Finjan contends that a “multi-lingual language detector” *must be* present because the accused instrumentalities “include a vocabulary built of programming languages which allow [the accused instrumentality] to classify web content,” “use techniques such as Bayesian analysis and gibberish detection to look inside the header and payload of network traffic to detect any specific one of a plurality of programming language in which the incoming stream is written,” and “inspect[] a number of different file types that are written in a number of different programming languages.” Dkt. No. 111-14 at 48–49. Finjan acknowledges that its contentions refer to the performance of certain functions. *See* Dkt. No. 118 at 16 (“Finjan explicitly identified what functionality of the Accused Product it contends are the multi-lingual language detectors and states that they inspect the incoming content to determine the language.”). However, Finjan says that it also refers to specifically to the technology that is used to meet this limitation. *Id.* ("Finjan also describes the technology that the multi-lingual language detector uses . . . .").

Again, the problem is that Finjan does not identify what component constitutes the multi-lingual language detector; it only identifies the function it performs and how it performs that function. Finjan must amend its contentions to identify the component or components of the accused instrumentalities that constitute the multi-lingual language detector of claim 9. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed multi-lingual language detector with specificity.

2. "scanner instantiator"

The parties' dispute concerning Finjan's contentions for the "scanner instantiator" limitation is similar to their dispute concerning Finjan's contentions for the "multi-lingual language detector." By its own admission, Finjan attempts to identify the accused scanner instantiator in the accused instrumentalities by describing "its functionality . . . and what it instantiates." Dkt. No. 118 at 16–17.

Finjan must amend its contentions to identify the component or components of the accused instrumentalities that constitute the scanner instantiator of claim 9. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed scanner instantiator with specificity.

3. "a scanner for the specific programming language"

SonicWall says that Finjan's contentions do not actually identify a scanner that is specific to any programming language, as claim 9 requires. Dkt. No. 112 at 17–18. Finjan does not dispute that its disclosure must identify a scanner specific to a programming language. It argues that by describing how the scanners are specific to a programming language, it has sufficiently identified the claimed scanner. Dkt. No. 118 at 7 (quoting Dkt. No. 111-14 at 53, 54–55). This is not sufficient.

Finjan must amend its contentions to identify the component or components of the accused instrumentalities that constitute the scanner of claim 9. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed scanner with specificity.

4. "rules accessor" / "analyzer for dynamically detecting"

SonicWall argues that the "scanner" of claim 9 has five sub-components. *See* Dkt. No. 112 at 17–19. In fact, the scanner has only four sub-components: a rules accessor, a tokenizer, a parser, and an analyzer. Dkt. No. 1-10 at claim 9. SonicWall says that Finjan has not identified a scanner that includes these sub-components, nor has it identified components that map to the rules accessor or the analyzer. Dkt. No. 112 at 18–19. Finjan responds that its contentions include details of what the rules accessor and analyzer do, and argues that because Finjan has already identified the scanner of claim 9, SonicWall's complaint that Finjan has not identified the components embodying the rules accessor and the analyzer is mistaken. Dkt. No. 118 at 17–20.

The difficulty with Finjan's arguments is that its contentions are mostly limited to describing the functionality of the rules accessor and the analyzer; it does not identify which components in the accused instrumentalities meet these limitations. *Id.* The Court is not persuaded that the "nature of the technology" makes it impossible for Finjan to identify the infringing components. *See id.* at 20. If Finjan has the benefit of SonicWall's technical specifications and source code for the accused instrumentalities, it should be able to identify the components that meet these limitations with specificity. Finjan must amend its contentions to identify the component or components of the accused instrumentalities that constitute the rules accessor and analyzer of claim 9.

5. "notifier"

SonicWall says that the "notifier" is a sub-component of the "scanner for the specific language," and that Finjan does not identify any component in the accused instrumentalities that meets this limitation. Dkt. No. 112 at 19. Finjan correctly observes that the "notifier" is not part of the claimed scanner, but rather a separate claim element. Dkt. No. 118 at 20. SonicWall does not address the "notifier" limitation in its reply. *See* Dkt. No. 120.

Nevertheless, the Court observes that Finjan's contentions for the "notifier" rely on a description of what the notifier does, not what it is. *See* Dkt. No. 111-14 at 78–79. As Finjan does not identify the component or components of the accused instrumentalities that constitute the notifier, it must amend its contentions to remedy this problem.

E. ’844 Patent

The ’844 patent is directed to a system and method for attaching to a Downloadable a security profile generated according to a set of rules based on the Downloadable’s content. Dkt. No. 1-2. SonicWall challenges the adequacy of Finjan’s contentions for the “inspector” limitation of asserted claim 1 and the “first content inspection engine” of asserted claim 15, both of which are reproduced below:

> 1. A method comprising:
>
> receiving by an inspector a Downloadable;
>
> generating by the inspector a first Downloadable security profile that identifies suspicious code in the received Downloadable; and
>
> linking by the inspector the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.
>
> 15. An inspector system comprising:
>
> memory storing a first rule set; and
>
> a first content inspection engine for using the first rule set to generate a first Downloadable security profile that identifies suspicious code in a Downloadable, and for linking the first Downloadable security profile to the Downloadable before a web server makes the Downloadable available to web clients.

Id. at claims 1, 15.

SonicWall says that Finjan’s contentions for the “inspector” and “first content inspection engine” limitations do not adequately disclose Finjan’s theories of infringement. Specifically, SonicWall argues that Finjan’s contentions are confusing because they suggest that the accused Gateways instrumentalities are themselves the claimed inspector/first content inspection engine while also identifying many other distinct elements or combinations of elements *within* and *among* the Gateways that meet these limitations. Dkt. No. 112 at 19–20. In addition, for some of the purported inspectors in the Gateways, SonicWall argues that Finjan does not disclose how each purported “inspector” meets the necessary requirements of that limitation. *Id.* at 20. Finjan responds by clarifying that it is indeed accusing both the Gateways themselves, as well as elements within the accused instrumentalities. Finjan cites to its contentions about what the inspector and first content inspection engine do and refers to figures incorporated into the contentions. Dkt. No. 118 at 20–21.

The Court agrees that Finjan’s contentions for these limitations of claim 1 and claim 15 are confusing. Finjan must amend its contentions to make clear its different theories of infringement (i.e., Gateways as a whole versus individual components versus combinations). In addition, Finjan must amend its contentions to clearly indicate which component or components meet the claimed limitations. For the inspector limitation, Finjan must also disclose how it contends the accused product or component meets all necessary requirements of that limitation. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed inspector and first content inspection engine with specificity.

F. ’780 Patent

The ’780 patent is directed to a system and method for protecting a computer and a network from hostile Downloadables. Dkt. No. 1-4. Asserted claim 9 recites as follows:

> 9. A system for generating a Downloadable ID to identify a Downloadable, comprising:
>
> > a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and
> >
> > an ID generator coupled to the communications engine that fetches at least one software component identified by the one or more references, and for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

Id. at claim 9.

SonicWall says that claim 9 requires “an ID generator” that “fetches at least one software component identified by the one or more references” included in the Downloadable and “perform[s] a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID." Dkt. No. 112 at 22. SonicWall argues that Finjan's contentions do not identify which component in the accused instrumentalities performs these functions. Finjan responds that it has identified the functionality in SonicWall's products that meet the ID generator limitation. Finjan argues that it should not be required to provide "the exact name for the structure" because the infringing feature is "software related." Dkt. No. 118 at 22–23.

Finjan may not rely on a description of allegedly infringing functionality that closely tracks the claim language without identifying the component or feature that performs the claimed function. There is no exception for software-related inventions, particularly where, as here, it appears that Finjan has access to SonicWall's technical specifications and source code. *See, e.g.*, *Creagri, Inc. v. Pinnaclife, Inc, LLC*, No. 11-cv-06635-LHK-PSG, 2012 WL 5389775, at *2 n.6 (N.D. Cal. Nov. 2, 2012) ("Where the accused instrumentality includes computer software based upon source code made available to the patentee, the patentee must provide 'pinpoint citations' to the code identifying the location of each limitation."); *Digital Reg*, 2013 WL 3361241, at *3–4 (requiring plaintiff to amend its infringement contention in part because it "has had access to [defendant's] source code [for eight months] and, at this juncture, should be able to amend its [infringement contentions] to clearly articulate how each of [defendant's] particular products infringe on Plaintiff's respective patents"); *Finjan, Inc. v. Sophos, Inc.*, No. 14-cv-01197-WHO, 2015 WL 5012679, at *3 (N.D. Cal. Aug. 24, 2015) (rejecting Finjan's argument that it was not required to provide pinpoint source code citations in its amended infringement contentions asserting the '780, '154, '926, '844, and '494 patents, among others). Finjan must amend its contentions to identify the component or components that meet the ID generator limitation of claim 9.

G. '154 Patent

The '154 patent is directed to a system and method for inspecting dynamically generated executable code. Dkt. No. 1-7. SonicWall challenges the adequacy of Finjan's contentions for several limitations of asserted claims 1, 3 and 10.

1. Claim 1: "first function" / "second function"

Asserted claim 1 recites:

> 1. A system for protecting a computer from dynamically generated malicious content, comprising:
>
> > a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;
> >
> > a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and
> >
> > a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

Dkt. No. 1-7 at claim 1.

SonicWall argues that claim 1 requires receiving content that includes "a call to a first function . . . the call including an input," followed by "transmitting the input to the security computer for inspection, when the first function is invoked," and thereafter "invoking a second function with the input, only if a security computer indicates that such invocation is safe." Dkt. No. 112 at 23–24. SonicWall's principle complaint is that Finjan's contentions do not identify a "first function" or "second function" that meets these limitations of claim 1. Finjan responds that it has disclosed the infringing "first function" in its contentions for the separate "content processor" limitation as follows:

> An example of first functions in the form of JavaScript functions include eval, unescape and document.write functions. For example, eval functions such as eval(base64_decode…) and eval(gzinflate…) are used to obfuscate or conceal automatic downloads of malware from a suspicious link or URI (e.g. malicious JavaScript, shellcode, drivebydownload, droppers, installers, malicious binary).

Dkt. No. 111-26 at 1; *see also id.* at 2 ("Another example of first function is 'unescape()' with a large amount of escaped data is detected. . . . An example of first functions in the form of a 'document.write()' function include document.write(unescape([obfuscated code])), where the first function is a document.write()."); *id.* at 3 ("Other examples of first functions are functions within PDFs for specifying the action to be performed automatically when the document is viewed such as downloading malware from a suspicious link or URL (e.g. OpenAction); Embed or Launch

SWF functions within a PDF for running an embedded video file; and functions for launching JavaScript within a PDF (e.g. Launch).”). Similarly, Finjan says that it has disclosed the infringing “second function” in its contentions for the separate “content processor” limitation as follows:

> Examples of second functions include recursive or suspicious scripts for obfuscating malicious links/URIs such as eval, unescape and document.write. In the following example, eval(base64_decode('ZXJyb3JfcmVwb3J0aW5nKDApOw0KJGJvd CA 9IE…)) is a second function that is recursively decoding the obfuscated code “ZXJyb3JfcmVwb3J0aW5nKDApOw0KJGJvdCA9IE…” Indirect calls to eval referencing the local scope of the current function or of unimplemented features (e.g. the document.lastModified property) are further examples of second functions.

Id. at 3. And, additionally:

> Second functions are typically a subsequent function that causes a download from the same URL such as connecting to or download files from a remote command and control (CnC) server using HTTPSendRequest, InternetReadFile with the input (e.g. URL, IP, file). The content processor will invoke a second function (e.g. HTTPS file download) with the input (e.g. URL) if the security computer indicates that such invocation is safe. These second functions will be invoked by the Accused Products.
>
> Second functions include sending results to a protected computer for automatically downloading from an obfuscated remote location and/or launching concealed input using certain combinations of JavaScript, iFrame injections and/or PDF (e.g. OpenAction or Launch). Such examples include JavaScript and OpenAction functions within PDFs for launching or downloading code for exploiting vulnerabilities within Adobe Reader and Adobe Acrobat such as malicious JavaScript, shellcode, drive-by download, droppers, installers and malicious binaries. Examples of such functions include URLDownloadToFile() for dropping malicious binaries; heap spraying functions including memory-related functions using PROCESS_MEMORY_COUNTERS; JavaScript functions in PDF for connecting to the Internet or making a network connection such as app.mailmsg() and app.launchURL(), as well as CONNECT-related and LISTEN-related functions; functions for executing malware via DLL injection such as CreateRemoteThread(); and functions for executing dropped malware, such as NtCreateProcess().

Id. at 4.

As explained above, Finjan’s use of “examples” renders its contentions open-ended and indefinite. However, the examples themselves are sufficiently disclosed with respect to the “first function" and "second function." Finjan should amend its contentions to ensure the contentions are complete and do not rely merely on examples; otherwise, Finjan risks being limited to the examples actually disclosed.

It is not clear, however, how Finjan believes the accused instrumentalities meet the further requirements of claim 1 of "transmitting the input to the security computer for inspection, when the first function is invoked," and thereafter "invoking a second function with the input." Here, Finjan appears to rely on contentions that essentially repeat the claim language. Finjan must amend its contentions to identify the basis for its view that the accused instrumentalities meet these other limitations of claim 1.

2. Claim 10: "computing device . . . receiv[ing] a modified input variable"

Asserted claim 10 is similar to claim 1 except that it discloses program code that additionally requires "receiv[ing]" and "calling a second function" with "a modified input variable" that "is obtained by modifying the input variable if the inspection of the input variable indicates that calling a function with the input variable may not be safe." Dkt. No. 1-7 at claim 10. SonicWall says that Finjan's contentions for claim 10 do not adequately specify how the identified program code causes a "computer device" to "receive a modified input variable." Dkt. No. 112 at 24. Finjan responds that it "does not have to explain what modifies the code or how it is modified . . . because that is not what the claim requires" and that it is sufficient that Finjan simply assert that Capture ATP is a computing device that "receive[s] a modified input variable." Dkt. No. 118 at 24.

Finjan identifies "modified code/parameters" as the "modified input variable" and describes "[t]he modified input variable being modified by code, parameters, or URLs." Dkt. No. 111-26 at 22. Finjan then cites to two SonicWall documents that generally describe the overall architecture and process of the Sandbox feature. *Id.* at 23–24. However, SonicWall contends (and Finjan does not dispute) that those documents say nothing about any kind of "modified code/parameters," or even any "code, parameters, or URLs." While Finjan is not required to explain how the input variable is modified, it must provide the bases for its existing contention, including accurate citations to evidence. *See, e.g.*, *Check Point*, 2019 WL 955000, at *5 ("If the cited materials contain information necessary to understand Finjan's infringement theories, Finjan must identify the particular supporting language in those sources and explain how that language fits into Finjan's theory of infringement.") (citing *Proofpoint*, 2015 WL 151720, at *6). Accordingly, Finjan must amend its contentions to identify the evidence on which it relies for this aspect of its contentions.

3. Claim 3: "the input is dynamically generated by said content processor prior to being transmitted by said transmitter"

Asserted claim 3 requires that the "input" to the "content processor" of claim 1 be "dynamically generated by said content processor prior to being transmitted by said transmitter." Dkt. No. 1-7 at claim 3. SonicWall points out that Finjan's contentions for claim 3 appear to assume that the "content processor" of claim 1 (from which claim 3 depends) is the same as the "security computer" also recited in claim 1. Dkt. No. 112 at 24–25. For this reason, SonicWall argues, Finjan has not provided a coherent theory of infringement for claim 3. Finjan does not respond directly to SonicWall's argument about the apparent disconnect between Finjan's contention and the claim language. *See* Dkt. No. 118 at 24–25.

Finjan must amend its contentions to address the ambiguity SonicWall identifies in its contentions for claim 3.

H. '968 Patent

The '968 patent is directed to a policy-based cache manager, which contains a memory storing a cache of digital content, policies, a policy index indicating allowable cache content, a content scanner to scan received digital content to derive a content profile, and a content evaluator to determine whether the content is allowable based on the profile. Dkt. No. 1-11. Asserted claim 1 of the '968 patent and its dependent claims 7 and 11 require a "policy based cache manager," comprised of, among other things, "a memory storing a cache of digital content, a plurality of policies, and a policy index to the cache contents." *Id.* at claims 1, 7, 11. The policy index "include[es] entries that relate cache content and policies by indicating cache content that is known to be allowable relative to a given policy, for each of a plurality of policies." *Id.*

SonicWall argues that Finjan's contentions do not identify any component of the accused instrumentalities that constitutes a "policy index to the cache contents" "including entries that relate cache content and policies by indicating cache content that is known to be allowable relative to a given policy." Dkt. No. 112 at 25. Finjan's contentions include the following disclosure:

> SonicWall Gateways include memory that saves collections of data locally that can be shared throughout a network of users or for further security processing. This data includes web content cached in memory, policies containing layers with one or more rules, and a policy index to the cache contents. This data is indexed by policy identifiers using the policy manager, which performs policy evaluation decisions using various policy constructs which include conditions, properties, rules and actions that relate cache content and policies by indicating cache content that is known to be allowable relative to a given policy, for each of a plurality of policies. When a browser request is received, SonicWall Gateways check the policy to determine if the cached content is known to be allowable. When the objects or collections of data crosses the network, a permission check occurs using the policy manager containing an index of entries that relate cached content and policies by indicating the allowability of certain cached content based on various set of rules against determinations concerning whether or not they have malware.

Dkt. No. 111-30 at 6–7. It appears that Finjan has identified allegedly infringing functions performed by the accused instrumentalities and so infers the existence of the claimed policy index. However, the contentions do not identify a component in the accused instrumentalities that constitutes the policy index. Instead, Finjan refers to an undefined "policy manager"—a term that SonicWall says does not appear in the cited documents—which either performs the indexing of cache contents or contains the index itself. *Id.* at 6–7.

Finjan must amend its contentions to identify the component or feature that performs that functions that it says the accused instrumentalities perform. If SonicWall has already produced technical specifications and source code for the accused instrumentalities, Finjan should be able to identify the claimed policy-based cache manager that meets the requirements of claims 1, 7, and 11.

I. Source Code

Finjan observes that the "infringing functionalities commonly reside in in the source code or in highly confidential internal technical documentation that is not made publicly available." Dkt. No. 118 at 4. As noted above, the parties agree that SonicWall has produced to Finjan technical documents, including source code accompanied by internal source code architecture documents and file manifests, although it is not clear from the record whether Finjan has access to this material for all accused instrumentalities.   In these circumstances, the patent holder generally is expected to cite to such documentation and source code in its infringement contentions. *Creagri*, 2012 WL 5389775, at *2 n.6 ("Where the accused instrumentality includes computer software based upon source code made available to the patentee, the patentee must provide 'pinpoint citations' to the code identifying the location of each limitation."); *Digital Reg*, 2013 WL 3361241, at *3–4 (requiring plaintiff to amend its infringement contention in part because it "has had access to [defendant's] source code [for eight months] and, at this juncture, should be able to amend its [infringement contentions] to clearly articulate how each of [defendant's] particular products infringe on Plaintiff's respective patents"); *see also Check Point*, 2019 WL 955000, at *6–7 (requiring Finjan to amend its infringement contentions with pinpoint source code citations); *Sophos*, 2015 WL 5012679, at *3 (same).

At the hearing, Finjan requested that the Court order SonicWall to produce a corporate representative for a Rule 30(b)(6) deposition on SonicWall's source code prior to any deadline for serving further supplemental contentions. SonicWall objects to such deposition on the ground that it is premature, given Finjan's failure to disclose its infringement contentions based on the information it already has. The Court is not persuaded that Finjan should be allowed to depose a corporate witness before it has crystallized its infringement theories. Dkt. No. 120 at 2.

IV. CONCLUSION

For the foregoing reasons, the Court grants SonicWall's motion to compel further infringement contentions as described above. Finjan shall serve its amended contentions no later than 30 days from the date of this order.

IT IS SO ORDERED.

Dated: May 1, 2019

Virginia K. DeMarchi

VIRGINIA K. DEMARCHI
United States Magistrate Judge